

## DETAILED ACTION

1. Currently pending claims are 1 – 16.

### *Response to Arguments*

2. Applicant's arguments with respect to instant claims have been fully considered but are moot in view of the new ground(s) of rejection necessitated by Applicant's amendment.

### *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1 – 14 and 16 are rejected under 35 U.S.C. 102(e) as being anticipated by Revital et al. (U.S. Patent 2004/0101138), which is incorporated by reference with Tsuria (U.S. Patent 6,178,242).

As per claim 1, Revital teaches an apparatus for processing a signal comprising:

**an input operable to receive the signal, the signal including a stream of encrypted data and a plurality of individually identified streams of messages, each of the individually identified streams of messages operable to be used to decrypt a common**

**part of the encrypted data independently of any other of the individually identified streams of messages** (Revital: Para [0010] Line 6 – 23: (a) Revital discloses a stream of SDSEG (digitally scrambled / encrypted digital data segment) (i.e. encrypted data) and a plurality of individually identified streams of ECM messages and TECM (Transformed ECM messages) (b) both ECM message and TECM message (using ECM key and TECM key respectively) can derive the same content key (i.e. control word) to decrypt the same /common encrypted data because the encrypted data on both cases are indeed scrambled with the same control word (i.e. content key) regardless either ECM or TECM key used based on ECM or TECM message – This matches decrypting a common part of the encrypted data independently of any other of the individually identified streams of messages – i.e., provide the same control word for use in decryption of a same portion of the stream of encrypted data regardless the use of live mode or re-play mode);

**a storage device coupled to the input for storing and retrieving the signal or part of the signal** (Revital: Para [0169] and Page 18 / left Column / Line 1 – 7 & Figure 5);

**a mode selection unit arranged to provide an output indicating a selection of an operating mode of a plurality of operating modes, the indicated selection of the operating mode associated with a particular one of the plurality of individually identified streams of messages that is to be used to for the selected operating mode in the decryption of the stream of encrypted data** (Tsuria : Figure 1 / Element 110, Column 9 Line 30 – 36, Column 3 Line 25 – 29 and Column 5 Line 1 – 9: there are two modes can be selected to operate either from a live rendering signal (i.e. performed on a direct broadcast SDDS (Scrambled Digital Data System) or from a stored play-back signal (i.e. performed on a replay of a recording SDDS from the digital VCR) through the IRD (Integrated Receiver Decoder) by using ECM key or TECM key associated with ECM or TECM messages respectively) & (Revital: Para [0068] Line 10 – 17,

Para [0010] and Figure 1: a mode selection unit selecting the proper mode (such as play-back mode other than the direct / liveTV-display mode) with an unique permission code from the broadcaster and using TECM and ECM message / key respectively to decrypt the scrambled data encrypted by the same content key (CW)); and

**a conditional access decoder coupled to the mode selection unit, to the input, and to the storage device, the conditional access decoder operable to receive the output indicating the selection of the operation mode, and to decrypt the encrypted data using a the particular one of the plurality of individually identified streams of messages associated with the selected operating mode, if entitled to use the particular one of the individually identified streams of messages, to generate a stream of decrypted data from the stream of encrypted data** (Revital: Para [0068] Line 10 – 17, Para [0010] and Figure 1: a mode selection unit selecting the proper mode (such as play-back mode other than the direct / liveTV-display mode) with an unique permission code from the broadcaster and using TECM and ECM message / key respectively to decrypt the scrambled data encrypted by the same content key (CW)) & (Tsuria : Figure 1 / Element 110, Column 9 Line 30 – 36, Column 3 Line 25 – 29 and Column 5 Line 1 – 9: the IRD (Integrated Receiver Decoder) can decrypt the encrypted data by using ECM key or TECM key associated with ECM or TECM messages respectively depending on the selected mode either from a direct / live TV rendering signal (i.e. performed on a direct broadcast SDDS (Scrambled Digital Data System) or from a stored play-back signal (i.e. performed on a replay of a recording SDDS from the digital VCR).

As per claim 5 and 6, the claim limitations are met as the same reasons as that set forth in the paragraph above regarding to claim 1 with the exception of the feature **distributing authorization information to one or more receivers of the signal** (Revital: Para [0068] Line

10 – 17, Para [0010] and Figure 1: a mode selection unit selecting the proper mode (such as play-back mode other than the direct / liveTV-display mode) with an unique permission code from the broadcaster and using TECM and ECM message / key respectively to decrypt the scrambled data encrypted by the same content key (CW)) & (Tsuria : Figure 1 / Element 110, Column 9 Line 30 – 36, Column 3 Line 25 – 29 and Column 5 Line 1 – 9: the IRD (Integrated Receiver Decoder) can decrypt the encrypted data by using ECM key or TECM key associated with ECM or TECM messages respectively depending on the selected mode either from a direct / live TV rendering signal (i.e. performed on a direct broadcast SDDS (Scrambled Digital Data System) or from a stored play-back signal (i.e. performed on a replay of a recording SDDS from the digital VCR), **including providing each one or more of the receivers with a selected authorization, the authorization being selected from a set of authorizations that includes at least one authorization to use combinations of the streams of messages to decrypt the stream of encrypted data, the authorization being selected in any given one of the receivers depending on availability in the given receiver of respective entitlements for respective ones of the authorizations** (same as above).

As per claim 2, Revital teaches the storage device being arranged to block out from the signal, during storage of the signal, at least one of the streams of messages other than the stream of messages that the conditional access decoder selects in the replay mode (Revital: Para [0068] Line 10 – 17, Para [0010] and Figure 1: a mode selection unit selecting the proper mode (such as play-back mode other than the direct / liveTV-display mode) with an unique permission code from the broadcaster and using TECM and ECM message / key respectively to decrypt the scrambled data encrypted by the same content key (CW)) & (Tsuria : Figure 1 / Element 110, Column 9 Line 30 – 36, Column 3 Line 25 – 29 and Column 5 Line 1 – 9: the IRD

Art Unit: 2131

(Integrated Receiver Decoder) can decrypt the encrypted data by using ECM key or TECM key associated with ECM or TECM messages respectively depending on the selected mode either from a direct / live TV rendering signal (i.e. performed on a direct broadcast SDDS (Scrambled Digital Data System) or from a stored play-back signal (i.e. performed on a replay of a recording SDDS from the digital VCR)).

As per claim 3, Revital teaches the decoder being arranged to detect the selected operating mode from the presence or absence of the at least one of the streams of messages that is blocked out from the signal during storage (Revital: Para [0068] Line 10 – 17, Para [0010] and Figure 1: a mode selection unit selecting the proper mode (such as play-back mode other than the direct / liveTV-display mode) with an unique permission code from the broadcaster and using TECM and ECM message / key respectively to decrypt the scrambled data encrypted by the same content key (CW)) & (Tsuria : Figure 1 / Element 110, Column 9 Line 30 – 36, Column 3 Line 25 – 29 and Column 5 Line 1 – 9: the selected operating mode is detected from the absence of the ECM messages of the streams that is blocked out from the signal during storage – i.e. detected from the presence of the TECM messages stored / recorded in the digital VCR playback device).

As per claim 4, Revital teaches a transcoder, the plurality of modes including a transcoding mode, the apparatus being arranged to transcode the signal when the operating mode selection unit selects the transcoding mode (Tsuria : Figure 1 / Element 130, Column 9 Line 30 – 36, Column 3 Line 25 – 29 and Column 5 Line 1 – 9: transcoding is considered as the technique of transforming multimedia content (e.g., text, images, audio, video and the like) from a first original format, in which the multimedia content was encoded, into a second format and

therefore the transformation of the signal format from the SDDS broadcast format into SDDS recording format, as shown in Figure 1, is indeed to arranged the transcoding of the signal based on the mode selection unit either using a live rendering signal (i.e. performed on a direct broadcast SDDS (Scrambled Digital Data System) or using a stored play-back signal (i.e. performed on a replay of a recording SDDS from the digital VCR) with the transcoding of the first SDDS broadcast format into the second SDDS recording format) & (Revital: Para [0068] Line 10 – 17, Para [0010] and Figure 1: a mode selection unit selecting the proper mode (such as play-back mode other than the direct / liveTV-display mode) with an unique permission code from the broadcaster and using TECM and ECM message / key respectively to decrypt the scrambled data encrypted by the same content key (CW)).

As per claim 7, Revital teaches the operating modes include a live rendering mode, wherein in the live rendering mode the mode selection unit provides one or more commands so that the signal provided at the input is passed to the conditional access decoder (Tsuria : Figure 1 / Element 110, Column 9 Line 30 – 36, Column 3 Line 25 – 29 and Column 5 Line 1 – 9) & (Revital: Para [0068] Line 10 – 17, Para [0010] and Figure 1: a mode selection unit selecting the proper mode (such as play-back mode other than the direct / liveTV-display mode) with an unique permission code from the broadcaster and using TECM and ECM message / key respectively to decrypt the scrambled data encrypted by the same content key (CW)).

As per claim 8, Revital teaches only the particular one of the plurality of individually identifiable streams of messages that is associated with the live rendering mode is used to decrypt the stream of encrypted data included in the signal provided at the input and passed on to the conditional access decoder for decryption during the live rendering mode

(Tsuria : Figure 1 / Element 110, Column 9 Line 30 – 36, Column 3 Line 25 – 29 and Column 5 Line 1 – 9) & (Revital: Para [0068] Line 10 – 17, Para [0010] and Figure 1: a mode selection unit to select the proper mode (such as play-back mode other than the direct / liveTV-display mode using TECM and ECM message / key respectively to decrypt the scrambled data encrypted by the same content key (CW)).

As per claim 9, Revital teaches the operating modes include a reply mode, wherein in the replay mode, the mode selection unit provides one or more commands so that the signal stored in the storage device is retrieved and passed to the conditional access decoder (Revital: Para [0068] Line 10 – 17, Para [0010] and Figure 1: a mode selection unit to select the proper mode (such as play-back mode other than the direct / liveTV-display mode using TECM and ECM message / key respectively to decrypt the scrambled data encrypted by the same content key (CW)) & (Tsuria : Figure 1 / Element 110, Column 9 Line 30 – 36, Column 3 Line 25 – 29 and Column 5 Line 1 – 9).

As per claim 10, Revital teaches only the particular one of the plurality of individually identifiable streams of messages that is associated with the reply mode is used to decrypt the stream of encrypted data included in the signal provided by the storage device and passed on to the conditional access decoder for decryption during the reply mode (Revital: Para [0068] Line 10 – 17, Para [0010] and Figure 1: a mode selection unit to select the proper mode (such as play-back mode other than the direct / liveTV-display mode using TECM and ECM message / key respectively to decrypt the scrambled data encrypted by the same content key (CW)) & (Tsuria : Figure 1 / Element 110, Column 9 Line 30 – 36, Column 3 Line 25 – 29 and Column 5 Line 1 – 9).

As per claim 11, Revital teaches a rendering unit coupled to the conditional access decoder, the rendering unit operable to render the stream of decrypted data provided by the conditional access decoder (Revital: Para [0068] Line 10 – 17, Para [0010] and Figure 1: a mode selection unit to select the proper mode (such as play-back mode other than the direct / liveTV-display mode using TECM and ECM message / key respectively to decrypt the scrambled data encrypted by the same content key (CW)) & (Tsuria : Figure 1 / Element 110, Column 9 Line 30 – 36, Column 3 Line 25 – 29 and Column 5 Line 1 – 9).

As per claim 12, Revital teaches a multiplexer coupled to the mode selection unit, to the input, to the storage device, and to the conditional access decoder, the multiplexer operable to receive the output from the mode selection unit indicating the selection of the operating mode, and to pass the signal from the input to the conditional access decoder if the output selection is indicative of a live rendering mode, and to pass the signal provided from the storage device to the conditional access decoder if the output selection is indicative of a reply mode (Revital: Para [0068] Line 10 – 17, Para [0010] and Figure 1 & Tsuria : Figure 1 / Element 110, Column 9 Line 30 – 36, Column 3 Line 25 – 29 and Column 5 Line 1 – 9: the MUX of the IRD needs to determine to pass the signal from the live /broadcast input (i.e. live-mode) or to pass the signal provided from the recording device (i.e. re-play mode) to the display terminal / TV).

As per claim 13, Revital teaches the stream of encrypted data is divided into a plurality of successive time intervals, and wherein for each of the time intervals the encrypted data is encrypted in a different way and needs a different control word for decrypting the encrypted data included within each successive time interval, and wherein the streams of messages include at



least two different entitlement control messages each including the control word needed to decrypt the encrypted data for a respective one of the successive time intervals within which the at least two different entitlement control message are included (Revital: Para [0068] Line 10 – 17, Para [0010] and Para [0116] Line 15 – 30 & Figure 1: a “key period” is being tracked and a mode selection unit to select the proper mode (such as play-back mode other than the direct / liveTV-display mode using TECM and ECM message / key respectively to decrypt the scrambled data encrypted by the same content key (CW)) & (Tsuria : Figure 1 / Element 110, Column 9 Line 30 – 36, Column 3 Line 25 – 29 and Column 5 Line 1 – 9).

As per claim 14, Revital teaches each of the plurality of individually identifiable streams of messages include a plurality of entitlement control messages, each of the plurality of entitlement control messages associated with a different one of the authorizations, and each of the plurality of entitlement control messages operable to provide a same control word for use in decryption of a same portion of the stream of encrypted data (Revital: Para [0010] Line 6 – 23: (a) Revital discloses a stream of SDSEG (digitally scrambled / encrypted digital data segment) (i.e. encrypted data) and a plurality of individually identified streams of ECM messages and TECM (Transformed ECM messages) (b) both ECM message and TECM message (using ECM key and TECM key respectively) can derive the same content key (i.e. control word) to decrypt the same /common encrypted data because the encrypted data on both cases are indeed scrambled with the same control word (i.e. content key) regardless either ECM or TECM key used based on ECM or TECM message – This matches decrypting a common part of the encrypted data independently of any other of the individually identified streams of messages – i.e., provide the same control word for use in decryption of a same portion of the stream of encrypted data regardless the use of live mode or re-play mode).

As per claim 16, Revital teaches the authorization is included in one or more entitlement management messages (Revital: Para [0109]: EMM messages).

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Revital et al. (U.S. Patent 2004/0101138), in view of Benardeau et al. (U.S. Patent 6,904,522).

As per claim 15, Revital does not teach expressly each of the individually identified streams of messages include at least a first control word and a second control word, the first control word for decrypting the current data and within a same time interval as the current data within the stream of encrypted data, and the second control word for decrypting the encrypted data that begins within the stream of encrypted data when there is a change in the control word needed to decrypt the stream of encrypted data.

Benardeau teaches each of the individually identified streams of messages include at least a first control word and a second control word, the first control word for decrypting the current data and within a same time interval as the current data within the stream of encrypted data, and the second control word for decrypting the encrypted data that begins within the stream of encrypted data when there is a change in the control word needed to decrypt the

stream of encrypted data (Benardeau: Column 9 Line 32 – 39: During a broadcast transmission, the control word typically changes every few seconds, and so ECM messages are also periodically transmitted to enable the changing control word to be descrambled. For redundancy purposes, each ECM typically includes two control words: the present control word and the next control word).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Benardeau within the system of Revital because (a) Revital teaches, in a conditional access multimedia system, tracking a key period information to associate the respective ECM message that contains the decryption information of control words (Revital: Para [0116] Line 15 – 30, Para [0126] Line 6 – 9, Para [0127] Line 14 – 17 / Line 11 – 14 and Para [0068] Line 10 – 17) and (b) Benardeau teaches the reliable and effective use of ECM message regarding the embedded control word wherein the access criteria and control word are transmitted to an encrypting unit via the linkage where an ECM is generated, encrypted and transmitted on to the multiplexer and scrambler and during a broadcast transmission, the control word typically changes every few seconds, and so ECMs are also periodically transmitted to enable the changing control word to be descrambled. For redundancy purposes, each ECM typically includes two control words: the present control word and the next control word (Benardeau: Abstract Benardeau: Column 10 Line 25 – 39).

***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LONGBIT CHAI whose telephone number is (571)272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Longbit Chai/

Primary Examiner, Art Unit 2131

Longbit Chai Ph.D.  
Patent Examiner  
Art Unit 2131  
9/25/2008